(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-147270
(P2012-147270A)
(43)公開日　平成24年8月2日(2012.8.2)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 4/04	(2009.01)	H04Q	7/00	107	5H181
H04W 12/04	(2009.01)	H04Q	7/00	182	5J104
G08G 1/09	(2006.01)	G08G	1/09	H	5K067
H04L 9/08	(2006.01)	G08G	1/09	F	
		H04L	9/00	601C	

審査請求 未請求　請求項の数 7　OL　（全 10 頁）

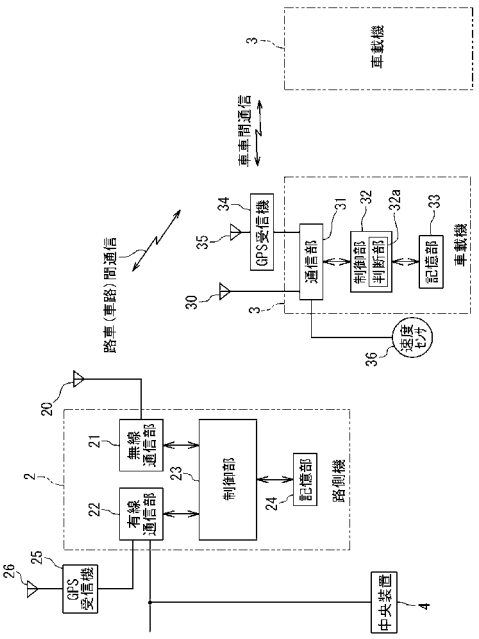
(21)出願番号　特願2011-4299(P2011-4299)
(22)出願日　平成23年1月12日(2011.1.12)

(71)出願人　000002130
住友電気工業株式会社
大阪府大阪市中央区北浜四丁目５番３３号
(74)代理人　110000280
特許業務法人サンクレスト国際特許事務所
(72)発明者　小河　昇平
大阪府大阪市此花区島屋一丁目１番３号
住友電気工業株式会社大阪製作所内

Fターム(参考)　5H181 AA01 BB04 FF05 FF13 FF27
5J104 AA16 AA32 AA34 EA04 EA15
EA16 JA03 NA02 NA37
5K067 AA30 AA33 BB21 CC08 DD17
DD51 EE02 EE06 EE25 HH22
HH23 HH36

(54)【発明の名称】通信システム及び通信方法

(57)【要約】
【課題】主として車載機における共通鍵の更新に、少なくとも積極的な契機を与え、確実な更新を推進する通信システム及び通信方法を提供する。
【解決手段】本発明は、道路交通における路側機２と車載機３との通信及び車載機３同士での通信に関して、データを共通鍵で暗号化することによりセキュリティを維持する通信システム又は通信方法であって、通信は、データを共通鍵で暗号化して行われ、車載機３は、自分が最新と認識する共通鍵のほかに、過去の共通鍵も記憶している。そして、車載機３は、通信相手からデータを受け取り、受け取ったデータを、最新と認識する共通鍵によって復調することを試み、復調できない場合、過去の共通鍵によって復調できるか否かの判断を行い、その判断結果に応じて少なくとも自他の共通鍵の相対的な新旧について判断する。
【選択図】図２



【特許請求の範囲】
【請求項１】
道路交通における路側機と車載機との通信及び車載機同士での通信に関して、データを共通鍵で暗号化することによりセキュリティを維持する通信システムであって、各車載機は、
データを前記共通鍵で暗号化して送信し又は復調して受信する通信部と、
自分が最新と認識する共通鍵のほかに、過去の共通鍵も記憶している記憶部と、
通信相手から受け取ったデータを、最新と認識する共通鍵によって復調できない場合、過去の共通鍵によって復調できるか否かの判断を行い、その判断結果に応じて少なくとも自他の共通鍵の相対的な新旧について判断する判断部と
を備えていることを特徴とする通信システム。
【請求項２】
前記判断部は、
前記過去の共通鍵によって復調できた場合は、前記通信相手の使用する共通鍵が、自分が最新と認識する共通鍵より古いと判断する第１の判断を行い、また、
前記過去の共通鍵によっても復調できない場合は、自分が最新と認識する共通鍵が前記通信相手の使用する共通鍵より古いと判断する第２の判断を行う、
請求項１記載の通信システム。
【請求項３】
前記第１の判断を行った場合の当該車載機は、前記通信相手に対して、共通鍵の更新の必要性を通知する請求項２記載の通信システム。
【請求項４】
前記第１の判断を行った場合の当該車載機は、前記通信相手に対して、自分が最新と認識する共通鍵を送信する請求項２又は３に記載の通信システム。
【請求項５】
前記第１の判断を行った場合の当該車載機は、自分の保有する最新の共通鍵について、当該共通鍵の利用が可能な期間である有効期間を取得しておりかつ当該有効期間を徒過している場合、その旨を前記通信相手に対して通知する請求項３又は４に記載の通信システム。
【請求項６】
前記第２の判断を行った場合の当該車載機は、前記通信相手に対して、最新の共通鍵の送信を要求する請求項２記載の通信システム。
【請求項７】
道路交通における路側機と車載機との通信及び車載機同士での通信に関して、データを共通鍵で暗号化することによりセキュリティを維持すべく、各車載機は、データを前記共通鍵で暗号化して通信するとともに、自分が最新と認識する共通鍵のほかに、過去の共通鍵も記憶していること、を前提とした通信方法であって、
通信相手からデータを受け取り、
受け取ったデータを、最新と認識する共通鍵によって復調することを試み、
復調できない場合、過去の共通鍵によって復調できるか否かの判断を行い、
その判断結果に応じて少なくとも自他の共通鍵の相対的な新旧について判断する
ことを特徴とする通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、高度道路交通システム（ＩＴＳ：Intelligent Transport System）におけるセキュリティを維持するための、通信システム及び通信方法に関する。
【背景技術】
【０００２】
近年、交通安全の促進や交通事故の防止を目的として、道路に設置されたインフラ装置

からの情報を受信し、この情報を活用することで車両走行の安全性を向上させる高度道路交通システムが検討されている（例えば、特許文献１参照）。

【０００３】

かかる高度道路交通システムは、主として、インフラ側の通信装置である複数の路側機と、道路を走行する各車両に搭載される無線通信装置である車載機とによって構成される。この場合、各通信主体間で行う通信の組み合わせには、路側機同士が行う路路間通信と、路側機と車載機とが相互に行う路車（又は車路ともいう。）間通信と、車載機同士が行う車車間通信とが含まれる。

【０００４】

ここで、路車間通信及び車車間通信では、例えば、悪意のある者が車載機になりすましてシステムに入り込む可能性がある。もし、これを許してしまうと、通信を混乱させる攻撃が行われる恐れがある。そこで、そのような事態を未然に防止するために、データの暗号化によるセキュリティの確保が必要である。一般に、暗号化方式としては例えば、共通鍵暗号方式や、公開鍵暗号方式が知られている。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特許第２８０６８０１号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

ここで、共通鍵方式では、何らかの方法で鍵を解読する者や不正な方法で鍵を入手する者に備えて、一定の期間等毎に更新することが望ましいと考えられる。その場合、路側機における共通鍵の更新は、インフラ側の管理下で行われるので、故障等の例外的事態を除き、基本的には確実に行われると考えることができる。しかしながら、車載機における共通鍵の更新は、車載機自身が、基本的には車両所有者の自主的管理に委ねられるので、必ずしも確実に更新されるとは限らない。車載機での共通鍵の更新が一定の確実性を持って行われなければ、路車間・車車間の通信が行えなくなる。

【０００７】

かかる課題に鑑み、本発明は、主として車載機における共通鍵の更新に、少なくとも積極的な契機を与え、確実な更新を推進する通信システム・通信方法を提供することを目的とする。

【課題を解決するための手段】

【０００８】

（１）本発明は、道路交通における路側機と車載機との通信及び車載機同士での通信に関して、データを共通鍵で暗号化することによりセキュリティを維持する通信システムであって、各車載機は、

データを前記共通鍵で暗号化して送信し又は復調して受信する通信部と、自分が最新と認識する共通鍵のほかに、過去の共通鍵も記憶している記憶部と、通信相手から受け取ったデータを、最新と認識する共通鍵によって復調できない場合、過去の共通鍵によって復調できるか否かの判断を行い、その判断結果に応じて少なくとも自他の共通鍵の相対的な新旧について判断する判断部とを備えたものである。

【０００９】

上記のような通信システムでは、路側機と車載機との間での路車間通信及び車載機同士での車車間通信は、共通鍵で暗号化されることによりセキュリティが維持され、例えば、悪意のある者が通信システムに入り込んで通信を混乱させる、というような事態は防止される。また、車載機は通信相手から受け取ったデータに基づいて、自分が最新と認識している共通鍵が、本当に最新か否かをチェックする機会を得るので、共通鍵の更新に、少なくとも積極的な契機を与えることができる。

【００１０】

（２）また、上記（１）の通信システムにおいて、判断部は、過去の共通鍵によって復調できた場合は、通信相手の使用する共通鍵が、自分が最新と認識する共通鍵より古いと判断する第１の判断を行い、また、過去の共通鍵によっても復調できない場合は、自分が最新と認識する共通鍵が通信相手の使用する共通鍵より古いと判断する第２の判断を行うようにすることができる。

この場合、過去の共通鍵を用いて復調できるか否かという簡易な手法により、どちらの方が古いかの判断を迅速的確に行うことができる。

【００１１】

（３）また、上記（２）の通信システムにおいて、第１の判断を行った場合の当該車載機は、通信相手に対して、共通鍵の更新の必要性を通知するようにしてもよい。

この場合、通信相手は、更新の必要性を知ることができる。また、「必要性」を通知するだけにとどめれば、最新の共通鍵が、当該通知によって洩れることもない。

【００１２】

（４）また、上記（２）又は（３）の通信システムにおいて、第１の判断を行った場合の当該車載機は、通信相手に対して、自分が最新と認識する共通鍵を送信してもよい。

この場合、通信相手は、自分の共通鍵が古かった場合に、当該車載機から新しい共通鍵を入手することができる。

【００１３】

（５）また、上記（３）又は（４）の通信システムにおいて、第１の判断を行った場合の当該車載機は、自分の保有する最新の共通鍵について、当該共通鍵の利用が可能な期間である有効期間を取得しておりかつ当該有効期間を徒過している場合、その旨を前記通信相手に対して通知することが好ましい。

この場合、通信相手は、自分の共通鍵が古かった場合に、当該車載機から新しい共通鍵を入手することができ、また、それが最新ではないという情報も併せて入手することができる。

【００１４】

（６）また、上記（２）の通信システムにおいて、第２の判断を行った場合の当該車載機は、通信相手に対して、最新の共通鍵の送信を要求するようにしてもよい。

この場合、当該車載機は、自分の共通鍵が古かった場合に、通信相手から新しい共通鍵を入手することができる。

【００１５】

（７）一方、本発明は、道路交通における路側機と車載機との通信及び車載機同士での通信に関して、データを共通鍵で暗号化することによりセキュリティを維持すべく、各車載機は、データを前記共通鍵で暗号化して通信するとともに、自分が最新と認識する共通鍵のほかに、過去の共通鍵も記憶していること、を前提とした通信方法であって、

通信相手からデータを受け取り、受け取ったデータを、最新と認識する共通鍵によって復調することを試み、復調できない場合、過去の共通鍵によって復調できるか否かの判断を行い、その判断結果に応じて少なくとも自他の共通鍵の相対的な新旧について判断する、というものである。

【００１６】

上記のような通信方法では、路側機と車載機との間での路車間通信及び車載機同士での車車間通信は、共通鍵で暗号化されることによりセキュリティが維持され、例えば、悪意のある者が通信システムに入り込んで通信を混乱させる、というような事態は防止される。また、車載機は通信相手から受け取ったデータに基づいて、自分が最新と認識している共通鍵が、本当に最新か否かをチェックする機会を得るので、共通鍵の更新に、少なくとも積極的な契機を与えることができる。

【発明の効果】

【００１７】

本発明の通信システム及び通信方法によれば、車載機における共通鍵の更新に、少なくとも積極的な契機を与えることができる。これにより、共通鍵の確実な更新を推進するこ

とができる。
【図面の簡単な説明】
【００１８】
【図１】本発明の実施形態に係る通信システム（及び通信方法）を含む、高度道路交通システムの全体構成における主要部のみを簡略に示す図である。
【図２】路側機と車載機の内部構成を示すブロック図である。
【図３】車載機が送信するデータフォーマットの一例を示す図である。
【図４】更新期間が不定期であり得る場合、言い換えれば更新期間が未知の場合について、鍵の更新に関する車載機の動作を示すフローチャートである。
【発明を実施するための形態】
【００１９】
《システムの全体構成》
図１は、本発明の一実施形態に係る通信システム（及び通信方法）を含む、高度道路交通システム（ＩＴＳ）の全体構成における主要部のみを簡略に示す図である。図１において、例えば道路脇に設置される支柱１には、道路側の通信機である路側機２が、取り付けられている。路側機２のアンテナ２０は、支柱１の上部に取り付けられている。車両Ａ，Ｂにはそれぞれ無線通信機である車載機（図１には図示せず。）が搭載され、アンテナ３０を備えている。
【００２０】
路側機２は、車載機との間での路車間通信を行うことができる。また、互いに通信可能な距離内にある車両Ａ，Ｂの車載機間で、例えばキャリアセンス方式により、車車間通信を行うことができる。なお、路側機２に対しては、交通管制センターの中央装置４から例えば有線で、信号の送受信が行われる。
各路側機２は、その周囲に広がるダウンリンクエリア（路側機２の送信信号が十分に届く範囲）をそれぞれ有し、自身のダウンリンクエリアを走行する車両の車載機に、ダウンリンク信号を受信させることができる。
【００２１】
各路側機２は、自装置が無線送信するためのタイムスロットをＴＤＭＡ方式で割り当てており、このタイムスロット以外の時間帯には無線送信を行わない。従って、路側機２用のタイムスロット以外の時間帯は、車載機のためのＣＳＭＡ方式による送信時間として開放されている。
また、路側機２は、自分の送信タイミングを制御するために他の路側機２との時刻同期機能を有している。この路側機２の時刻同期は、例えば、自分の時計をＧＰＳ時刻に合わせるＧＰＳ同期や、自分の時計を他の路側機２からの送信信号に合わせるエア同期等によって行われる。
【００２２】
《回路ブロック図の構成及び基本的通信動作》
図２は、路側機２と車載機３の内部構成を示すブロック図である。
路側機２は、主として、無線通信のためのアンテナ２０が接続された無線通信部２１と、中央装置４と双方向通信する有線通信部２２と、それらの通信制御を行うＣＰＵ等よりなる制御部２３と、制御部２３に接続されたＲＯＭやＲＡＭ等の記憶装置よりなる記憶部２４とを備えている。
【００２３】
路側機２の有線通信部２２には、前記中央装置４の他にも、ＧＰＳ受信機２５が接続されている。このＧＰＳ受信機２５は、ＧＰＳアンテナ２６により、複数のＧＰＳ衛星（図示せず。）からＧＰＳ信号を受信する。なお、ＧＰＳ受信機２５は、路側機２内に設けられるものであってもよい。
【００２４】
制御部２３は、有線通信部２２が受信した中央装置４からの交通情報等を、記憶部２４に一時的に記憶させ、無線通信部２１を介して自己のダウンリンクエリアにブロードキャ

スト送信することができる。但し、後述するが、セキュリティに関する情報は、ブロードキャストで送信しない方が好ましい。また、制御部２３は、無線通信部２１が受信した車載機３からの情報を、記憶部２４に一時的に記憶させ、有線通信部２２を介して中央装置４に転送することができる。

【００２５】

また、制御部２３は、記憶部２４に記憶されたタイムスロットの割当情報を、無線通信部２１を介して自己のダウンリンクエリアにブロードキャスト送信する。この割当情報は、路側機２の送信時間を車載機３に通知するためのものである。ダウンリンクエリアを走行する車両の車載機３は、路側機２が送信を行わない時間帯に、キャリアセンス方式による無線送信を行う。

【００２６】

一方、車載機３は、無線通信のためのアンテナ３０に接続された通信部３１と、この通信部３１に対する通信制御を行うＣＰＵ等よりなる制御部３２と、この制御部３２に接続されたＲＯＭやＲＡＭ等の記憶装置よりなる記憶部３３とを備えている。制御部３２は、セキュリティに関する後述の判断を行う判断部３２ａとしての機能も含んでいる。また、通信部３１には、ＧＰＳ受信機３４及び速度センサ３６が接続されている。ＧＰＳ受信機３４は、ＧＰＳアンテナ３５により、複数のＧＰＳ衛星（図示せず。）からＧＰＳ信号を受信する。なお、ＧＰＳ受信機３４は、車載機３内に設けられるものであってもよい。

【００２７】

車載機３の制御部３２は、車車間通信のためのキャリアセンス方式による無線通信を通信部３１に行わせるものであり、路側機２との間の時分割多重方式での通信制御機能は有していない。

従って、車載機３の通信部３１は、所定の搬送波周波数の受信レベルを常時感知しており、その値がある閾値以上である場合は無線送信を行わず、当該閾値未満になった場合にのみ無線送信を行うようになっている。

【００２８】

なお、車載機３の制御部３２は、車両（車載機３）の現時点の位置、方向、速度、車種等を含む車両情報を、通信部３１を介して無線送信することができる。また、車載機３の制御部３２は、他の車両から直接受信した情報や、路側機２から受信した他の車両の情報に含まれる、位置、速度及び方向に基づいて、右直衝突や出合い頭衝突等を回避するための安全運転支援制御を行うことができる。

【００２９】

《セキュリティに関する通信システム》

以上の、路車間通信及び車車間通信は、共通鍵で暗号化される。暗号化及び復調は、無線通信部２１及び通信部３１にて行われる。暗号化によって、例えば、悪意のある者が車載機になりすまして通信システムに入り込み、通信を混乱させる、というような事態を防止することができる。また、共通鍵は、安全上、逐次更新していく必要がある。このような更新は、不定期に行われる場合と、定期的に行われる場合とがあり得る。

【００３０】

図３は、車載機３（路側機２もほぼ同様である。）が送信するデータフォーマットの一例を示す図である。図において、車載機３の送信信号には、先頭から順に、Ｌ２（ＭＡＣ）ヘッダ、通信制御ヘッダ、セキュリティヘッダ、Ｌ７（アプリ制御）ヘッダ、アプリデータ、及び、セキュリティフッタが含まれている。このうち、セキュリティヘッダには、発信者ＩＤ、鍵ＩＤ、その他、車載機／路側機の識別ＩＤ、位置や時刻の情報、認証用乱数等が含まれている。なお、アプリデータにも位置や時刻の情報が含まれる場合があり、その場合には、こちらの情報を利用することも可能である。また、セキュリティフッタには、署名データが含まれている。

【００３１】

《共通鍵の更新：更新期間が不定期であり得る場合》

次に、共通鍵の更新について説明する。まず、更新期間（鍵の利用が可能な期間である

有効期間）が不定期であり得る場合、言い換えれば更新期間が未知の場合について、図４のフローチャートを参照して説明する。このフローチャートの処理は車載機３内の通信部３１、制御部３２（判断部３２ａ）、記憶部３３を用いて行われる。

【００３２】

各車載機３は、自分が最新と認識する共通鍵の他、更新前の過去の共通鍵も含めて複数世代分の鍵を記憶している。ここで、任意の１台の車両の車載機３を想定する。共通鍵の更新が不定期である場合には、頻繁に自分の共通鍵が最新のものであるか否かをチェックする必要がある。そこで、例えば定期的に、図４のフローチャートの処理を実行する。

【００３３】

まず、車載機３は、通信部３１で信号を受信するのを待つ（ステップＳ１でＮｏの繰り返し）。信号を受信すると、車載機３は、検波した受信レベルが、所定値以上の十分なレベル（振幅）であるか否かを判断し（ステップＳ２）、十分でないときはステップＳ１に戻って次の機会を待つ。受信レベルが十分であれば、通信部３１は、自分が最新と認識している鍵で暗号の復調を試みる（ステップＳ３）。この結果、復調ができれば、そのまま処理終了となる（ステップＳ４）。

【００３４】

しかし、ステップＳ４において復調ができないときは、更新前の、言い換えれば一世代前の鍵を記憶部３３から読み出し、この鍵を用いて再度復調を試みる（ステップＳ５）。この結果、復調ができれば（ステップＳ６のＹｅｓ）、相手は古い鍵を使っていた、ということになるので、信号を送信して来た相手の鍵が自分の鍵よりも古い、と判断する（ステップＳ７）。この判断結果となる場合の相手方は、主として車載機である。インフラ側にある路側機２の使用している鍵の方が古いということは、通常は極めて起こりにくいと考えられる。そして、この判断結果に基づいて、当該車載機３は、相手方に対して、鍵が古いと知らせる通知を行うか、又は、自分が所有している最新の鍵を与えるべく送信する、という処理を行う（ステップＳ８）。

【００３５】

なお、最新の鍵を与えるべく送信を行うのは、セキュリティを維持する共通鍵の情報が洩れるというリスクもあるので、その点では、鍵が古いと知らせる通知を行うことにとどめる方が安全ではある。また、いずれの場合も、相手が復調できる古い鍵を使って暗号化した信号（通知／鍵）を送ることが好ましい。

【００３６】

一方、上記ステップＳ６において復調ができなかったときは、自分の所有するいずれの鍵でも復調できなかった、ということになる。これはすなわち、自分が最新と認識していた鍵すら、もはや古い鍵である、ということになるので、車載機３は、信号を送信して来た相手の鍵よりも自分の鍵が古い、と判断する（ステップＳ９）。また、この判断結果に基づいて、車載機３は、例えばカーナビゲーション装置のディスプレイ（図示せず。）にその判断結果を表示し、又は、音声で知らせること等により、運転者への警告を行うことができる（ステップＳ１０）。

【００３７】

なお、上記ステップＳ７又はＳ９の判断によって、自分の鍵が古いと認識するか、又は、他の装置から「鍵が古い」という通知を受けた車載機については、例えば、車両の所有者がディーラー等に車載機を持ち込んで、上記の通信システムの運営者（警察等）から適法に有線経由で配布を受けた共通鍵の情報をもらうことにより、更新処理を行うようにしてもよい。

【００３８】

また、上記ステップＳ１０においては、相手方に対して、最新の鍵の送信を要求する信号を送る、という処理を行ってもよい。この場合、相手方（他の車載機又は路側機）は、最新の鍵を与えるべく送信を行うことになるが、セキュリティを維持する共通鍵の情報が洩れるというリスクもあるので、情報を受け取る車載機が復調できる古い鍵を使って暗号化した信号（最新の共通鍵）を送ることが好ましい。

【００３９】
なお、そのほか、路側機２から最新の共通鍵を車載機３に提供するには、共通鍵の情報洩れを防止するために、ブロードキャストではなく、一対一の送信を行うことが好ましい。
また、路側機２は、車載機３から提供の要求があった場合のみ、送信を行うべきであり、むやみに提供してはいけない。
また、送信電力を一定値以下に抑制して、他の車載機や不特定の受信者に情報が届きにくくすることが好ましい。
また、路側機２は、交通量を監視しておき、交通量の少ないときに、特定の車載機３をねらって送信することが好ましい。
また、車両に搭載された車載機以外の受信装置へ情報が洩れることを防止すべく、最新の共通鍵の提供を求めた車載機が移動していることを確認した場合にのみ、情報を提供するようにしてもよい。
【００４０】
なお、図４のフローチャートでは、ステップＳ５の処理は１回のみであるように説明したが、これは一例に過ぎない。すなわち、更新前の鍵で復調を試みるのは、一世代前の鍵には必ずしも限定されないので、記憶している複数世代をさかのぼるように順に、復調を試みてもよい。例えば、最新の鍵を含めて３世代分以上の所定数の種類の鍵を記憶しておき、復調できるまで逐次古い鍵を試す、という処理を行ってもよい。
【００４１】
以上のような通信システムでは、路車間通信及び車車間通信は、共通鍵で暗号化されることによりセキュリティが維持され、例えば、悪意のある者が通信システムに入り込んで通信を混乱させる、というような事態は防止される。また、車載機３は通信相手から受け取ったデータに基づいて、自分が最新と認識している共通鍵が、本当に最新か否かをチェックする機会を得るので、共通鍵の更新に、積極的な契機を与えることができる。また、これに基づいて、共通鍵の確実な更新を推進することができる。
また、過去の共通鍵を用いて復調できるか否かという簡易な手法により、どちらの方が古いかの判断を迅速的確に行うことができる。
【００４２】
《参考例としての共通鍵の更新：更新期間が定期的である場合》
次に、参考例として、共通鍵の更新が定期的に行われる場合の車載機３の対応について説明する。この場合の処理は、図４のフローチャートとは全く別である。
（ｉ）まず、車載機３は、予め決まっている更新期間（有効期間）ｔｒの情報を取得している。そして、車載機３は、鍵を更新してから現時点までの経過時間ｔを、更新期間ｔｒと比較して、自分の鍵が最新か否かを判断する。
（ｉｉ）そして、更新期間ｔｒに対する経過時間ｔの割合（ｔ／ｔｒ）が所定値（例えば０．９）以上になると、カーナビゲーション装置等を利用して、運転者に、更新の時期が近づいていることを知らせ、注意を促し続ける。
（ｉｉｉ）これを受けて、運転者は、鍵の更新ができる所定の場所（ディーラー等）に、車載機を搭載した車両を持ち込み、最新の鍵への更新を行う、という処理となる。
【００４３】
《その他》
なお、今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は特許請求の範囲によって示され、特許請求の範囲と均等の意味及び範囲内での全ての変更が含まれることが意図される。
【００４４】
例えば、共通鍵の更新を定期的に行うが、必要に応じて随時行うこともできる通信システムとしてもよい。
この場合、例えば、通信相手の鍵が古く、自分の方が新しいと判断した車載機が、自分の鍵を通信相手に送信する場合、実は、自分は共通鍵の最新の更新期間を徒過している、

という状況も起こり得る。このような場合には、その徒過の事実も併せて通信相手に通知するようにすれば、通信相手は、自分の共通鍵が古かった場合に、当該車載機から新しい共通鍵を入手することができ、また、それが最新ではないという情報も併せて入手することができる。

【符号の説明】

【００４５】

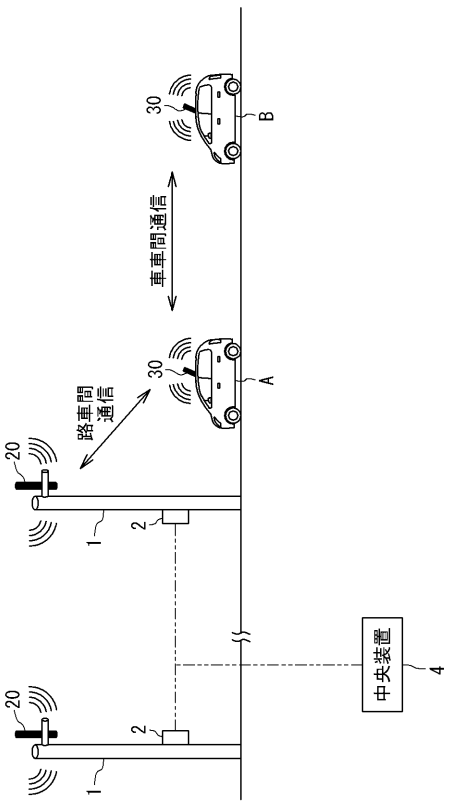
３：車載機

３１：通信部

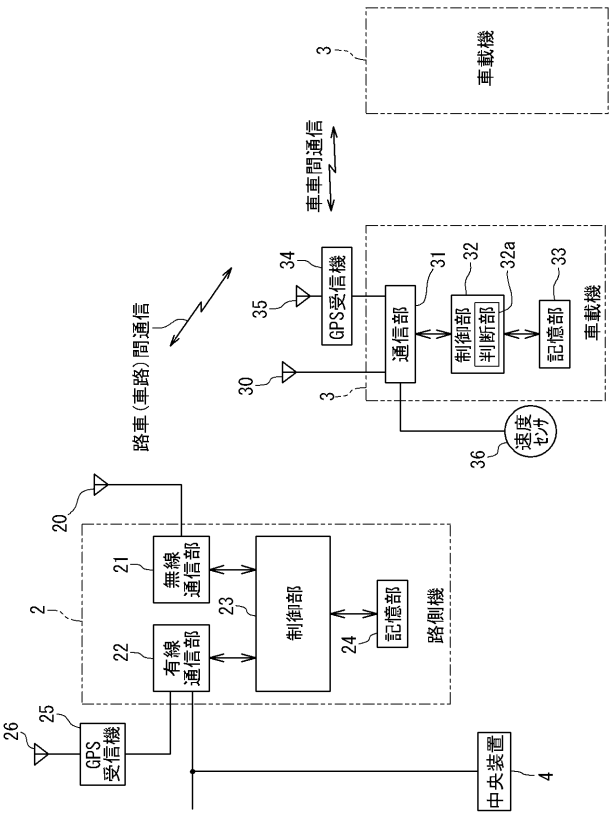
３２ａ：判断部

３３：記憶部

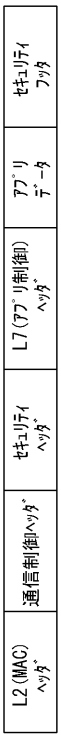
【図１】



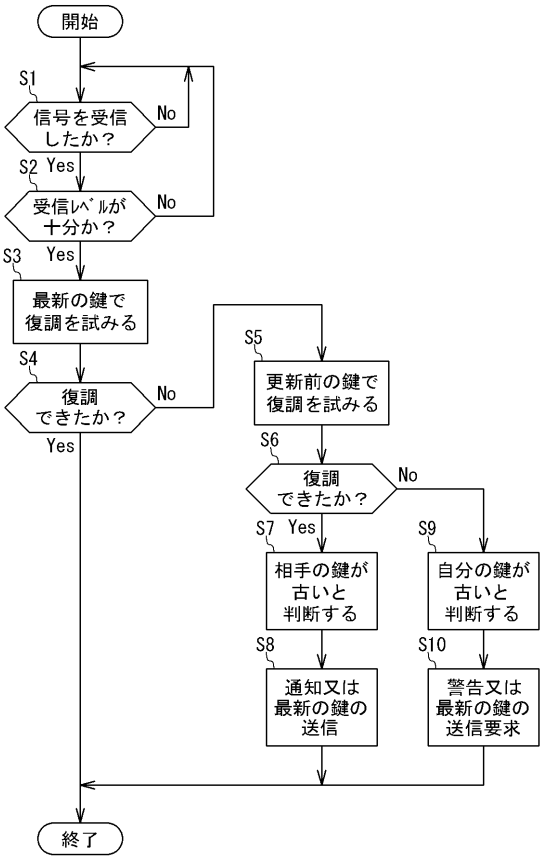
【図２】



【図３】


セキュリティ フッタ
アプリ データ
L7(アプリ制御) ヘッダ
セキュリティ ヘッダ
通信制御ヘッダ
L2(MAC) ヘッダ

【図４】


開始
S1
信号を受信したか？
No
S2
Yes
受信レベルが十分か？
No
S3
Yes
最新の鍵で復調を試みる
S4
復調できたか？
No
Yes
S5
更新前の鍵で復調を試みる
S6
復調できたか？
No
S7
Yes
相手の鍵が古いと判断する
S8
通知又は最新の鍵の送信
S9
自分の鍵が古いと判断する
S10
警告又は最新の鍵の送信要求
終了